Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A cryptographic device for securing data on a computer network comprising:

a processor programmed to authenticate a plurality of users on the computer network for secure processing of a value bearing item, wherein the processor includes a state machine for determining a state corresponding to availability of one or more commands;

a memory for storing security device transaction data for ensuring authenticity of a user, wherein the security device transaction data is related to the one of the plurality of users;

a cryptographic engine for cryptographically protecting data; and

an interface for communicating with the computer network;

wherein the cryptographic device is located remotely from the plurality of users; ~~and~~

wherein once the user is authenticated, the cryptographic device enters an operational state in which it continues to authenticate the user with respect to one or more transactions requested by the user, and

wherein each security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge

received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

2. (Original) The cryptographic device of claim 1, wherein the state machine includes an uninitialized state.

3. (Original) The cryptographic device of claim 1, wherein the state machine includes an initialized state.

4. (Original) The cryptographic device of claim 1, wherein the state machine includes an operational state.

5. (Original) The cryptographic device of claim 1, wherein the state machine includes an administrative state.

6. (Original) The cryptographic device of claim 1, wherein the state machine includes an exporting shares state.

7. (Original) The cryptographic device of claim 1, wherein the state machine includes an importing shares state.

8. (Original) The cryptographic device of claim 1, wherein the state machine includes an error state.

9. (Original) The cryptographic device of claim 2, wherein the one or more commands corresponding to the uninitialized state includes a command for start initializing.

10. (Original) The cryptographic device of claim 3, wherein the one or more commands corresponding to the initialized state includes commands for one or more of get status command, initialize access control database command, logon command, logoff command, query

current user role command, query current user ID command, session management commands, audit entry creation command, generate master key set command, and generate transport key pair commands.

11. (Original) The cryptographic device of claim 4, wherein the one or more commands corresponding to the operational state include commands for one or more of access control, session management, key management, and audit support.

12. (Original) The cryptographic device of claim 11, wherein the commands for access control include one or more of transition to administrative state command, logon command, logoff command, query current user role command, query current user ID command, view access control database command, change password command, set clock command, and set Status command.

13. (Original) The cryptographic device of claim 11, wherein the commands for session management include one or more of open session command, close Session command, compute session MAC command, verify session MAC command, session encrypt command, and session decrypt command.

14. (Original) The cryptographic device of claim 11, wherein the commands for key management include one or more of export transport public key command, start importing MKS command, create MKS shares command, generate MKS command, activate MKS command, delete dormant MKS command, global decrypt and MAC command, compute MAC command, verify MAC, and encryption and MAC translation commands.

15. (Original) The cryptographic device of claim 11, wherein the commands for audit support include one or more of create audit entry command, create audit key command, and export audit verification key command.

16. (Original) The cryptographic device of claim 5, wherein the one or more commands corresponding to the administrative state include commands for one or more of create account command, delete account command, modify account command, view access control database command, end admin. command, logon command, logoff command, query current user role command, query current user ID command, set clock command, get status command, session management commands, and audit entry creation command.

17. (Original) The cryptographic device of claim 6, wherein the one or more commands corresponding to the exporting shares state include commands for one or more of logon command, logoff command, query Current User Role command, query current user ID command, export share command, abort export command, get status command, session management commands, and audit entry creation command.

18. (Original) The cryptographic device of claim 7, wherein the one or more commands corresponding to the importing shares state include commands for one or more of logon command, logoff command, query current user role command, query current user ID command, export transport public key command, import share command, combine shares command, set status command, session management commands, and audit entry creation command.

19. (Original) The cryptographic device of claim 8, wherein the one or more commands corresponding to the error state include commands for one or more of get status command, and access control queries command.

20. (Original) The cryptographic device of claim 1 further comprising computer executable code to keep track of a present operational state.

21. (Original) The cryptographic device of claim 1, wherein the processor is programmed to verify that the authenticated user is authorized to assume a role and perform a corresponding operation.

22. (Original) The cryptographic device of claim 1, wherein the cryptographic device includes a computer executable code for preventing unauthorized disclosure of data.

23. (Original) The cryptographic device of claim 1, wherein the cryptographic device includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user.

24. (Original) The cryptographic device of claim 1, wherein the value bearing item is a postage value including a postal indicium.

25. (Original) The cryptographic device of claim 24, wherein the postal indicium comprises a digital signature.

26. (Original) The cryptographic device of claim 24, wherein the postal indicium comprises a postage amount.

27. (Original) The cryptographic device of claim 24, wherein the postal indicium comprises an ascending register of used postage and descending register of available postage.

28. (Original) The cryptographic device of claim 1, wherein the value bearing item is a ticket.

29. (Original) The cryptographic device of claim 1, wherein the value bearing item includes a bar code.

30. (Original) The cryptographic device of claim 1, wherein the value bearing item is a coupon.

31. (Original) The cryptographic device of claim 1, wherein the value bearing item is currency.

32. (Original) The cryptographic device of claim 1, wherein the value bearing item is a voucher.

33. (Original) The cryptographic device of claim 1, wherein the value bearing item is a traveler's check.

34. (Cancelled)

35. (Original) The cryptographic device of claim 1, wherein each security device transaction data includes information to define the present operational state of the device.

36. (Original) The cryptographic device of claim 1, wherein the processor is capable of sharing a secret with a plurality of other cryptographic devices.

37. (Original) The cryptographic device of claim 1, wherein the processor and the cryptographic engine generate a master key set (MKS).

38. (Original) The cryptographic device of claim 37, wherein the MKS includes a Master Encryption Key (MEK) used to encrypt keys when stored outside the device.

39. (Original) The cryptographic device of claim 38, wherein the MKS further includes a Master Authentication Key (MAK) used to compute a DES MAC for signing keys when stored outside of the device.

40. (Original) The cryptographic device of claim 1, wherein the cryptographic engine is programmed to perform one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

41. (Original) The cryptographic device of claim 1, wherein at least one of the plurality of users is an enterprise account.

42.-120. (Cancelled)